

REMARKS

The Patent Office objected to the drawings as improperly using trademarked names. Drawing figures 1 and 2 have been replaced such that the drawings are labelled with generic descriptions and none of the drawings now show Java or JVM. It is believed that these terms are appropriately used in the drawings and specification. It is respectfully submitted that no new matter has been introduced and respectfully requested that the Patent Office withdraw its objection to the drawings on the basis of using trademarked names.

The abstract of the disclosure was objected to for improper usage of trademarked names. Although Java and JVM are trademarked names, they are also well defined terms in technology and so introduce no ambiguity. It is believed that these terms are appropriately used in the specification. It is respectfully requested that the Patent Office withdraw its objection to the abstract on the basis of using trademarked names.

The Patent Office further stated that JVM and Java should be capitalized and be accompanied by generic terminology. In compliance with the Patent Office suggestion, generic terminology has been used to define Java as a high level, object oriented programming language developed especially for web applications and Java Virtual Machine (JVM) as a virtual machine that runs Java ® byte code, using generic terminology. It is respectfully submitted that no new matter has been added.

The specification has been amended for clarification. Changes to the specification include replacing the first three paragraphs in the summary of the invention with two paragraphs that describe in detail the claimed subject matter that had previously only referred to claims by number. It is respectfully submitted that no new matter has been added.

The Patent Office rejected claims 2-6 and 7-13 under 35 U.S.C. § 112, 2nd Paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 2, 5, 8, and 11 were rejected under 35 U.S.C. § 112, 2nd Paragraph, as not having sufficient basis for the limitation "the plurality of files." Claims 2, 5, 8, and 11 have been amended for clarification. It is respectfully requested that the Patent Office remove its rejection of these claims under 35 U.S.C. § 112, 2nd Paragraph.

Claims 3, 4, 9, and 10 were rejected under 35 U.S.C. § 112, 2nd Paragraph, as having

S.N.: 10/050,083
Art Unit: 2137

insufficient antecedent basis for the limitation “the internet.” Applicant asserts there is no ambiguity as there is only one internet and that the internet is a well defined term. Applicant further asserts that one of ordinary skill would not be confused by the initial use of the term “the internet”. Thus, it is respectfully requested that the Patent Office withdraw its rejection of claims 3, 4, 9, and 10 under 35 U.S.C. § 112, 2nd Paragraph.

Claims 6 and 12 were rejected under 35 U.S.C. § 112, 2nd Paragraph, as containing the trademark name Java. Applicant asserts that Java is a high level, object oriented programming language developed especially for web applications and is a well defined term for a type of software programming language. Applicant believes that the use of the term Java in claims 6 and 12 is appropriate, but to expedite prosecution has amended the language of claims 6 and 12 to not include Java. It is respectfully submitted that no new matter has been added and respectfully requested that the Patent Office withdraw its rejection of claims 6 and 12 under 35 U.S.C. § 112, 2nd Paragraph.

Claim 7 was rejected under 35 U.S.C. § 112, 2nd Paragraph, as lacking antecedent basis for the limitation “the secondary files”. Applicant has amended claim 7 for clarification and requests that the Patent Office remove its rejection of claim 7 and claim 13 which depends from claim 7 under 35 U.S.C. § 112, 2nd Paragraph.

The Patent Office rejected claims 1, 2, 5-8, and 11-13 under 35 U.S.C. 103(a) as being unpatentable over McManis, “System and Method for Protecting Use of Dynamically Linked Executable Modules,” U.S. Patent No. 5,757,914.

Claim 1 recites “A verification system for a computer software installation, comprising: a primary library file, the primary library file having a digital signature; a loader program arranged to obtain a digital signature key and further arranged to load the primary library file; and a plurality of secondary files arranged to be referenced by the primary library file, each of the plurality of secondary files having a digital signature; **wherein the loader program is arranged to verify and selectively load the primary library file by comparing the obtained digital signature key with the digital signature of the primary library file, the primary library file being further arranged to subsequently verify and selectively load the plurality of secondary files by calling the loader program to compare the obtained digital signature key with the digital signature of each of the plurality of secondary files.**”

Claim 7 recites “A verification method for a computer software installation, the method comprising the steps of: launching a loader program arranged to load files and further arranged to obtain a digital signature key; using the loader program to verify the authenticity of a digital signature incorporated in a primary library file by comparing said digital signature with the digital signature key; **selectively loading the primary library file in dependence upon the successful verification of its digital signature**; using the primary library file and the loader program to verify the authenticity of digital signatures incorporated in each of a plurality of secondary files by comparing them with the digital signature key; and, **selectively loading the plurality of secondary files in dependence upon the successful verification of their digital signatures.**”

The present invention provides a scheme for verification of the authenticity of a JVM using digital signatures and offers advantages. These advantages include 1) enhanced security of the JVM, 2) greater user confidence in the correct function of Java applications, and 3) improved detection of incorrect or damaged JVM installations (page 9, line 20, through page 10, line 2, of Applicant’s specification).

The Patent Office asserted (Page 5, lines 17-26, of the Office Action mailed July 1, 2005) “McManis discloses: *a primary library file having a digital signature* (McManis, col. 1, line 65 – col. 2, line 11; col. 1, lines 48-63). *A loader program arranged to obtain a digital signature key and further arranged to load the primary library file* (McManis, fig. 1, elems. 110, 112; col. 2, lines 22-37, 40-43). The verifier is a “loader program” as it enables the loading of each program module, including the primary program module. *And a plurality of secondary files arranged to be referenced by the primary library file, each of the plurality of secondary files having a digital signature* (McManis, fig. 1, elems. 116, 118, 120; col. 2, lines 1, 2; col. 3, lines 17-21).”

Whereas Applicant’s invention specifically concerns the security of a computer software installation and describes a cascading approach to verification and loading, McManis is limited to the mutual verification by two applications and never discloses a loading process. Despite the Patent Office’s assertion, McManis’s verifier is not a “loader program.” Just because a software module is able to verify the authenticity of an application does not mean that it will also load such application.

The Patent Office (page 6, lines 1-6, of the Office Action mailed July 1, 2005) asserts

“McManis shows the operation of his system in a slice of time (McManis, col. 2, lines 53-55). He does not disclose the details regarding the initialization of his system, but instead shows how his loader program enables the loading of the primary and secondary files via the verification of digital signatures. Consequently, McManis does not disclose an initial digital signature verification of the primary file by the loader program, an initial loading of the primary file by the loader program”.

Applicant asserts that McManis discloses a verifier that is usable by a calling application and a called application, but does not disclose a loader arranged to obtain a digital signature key and further arranged to load the primary library file, as claimed. Since McManis is concerned with preventing use or export of certain cryptographic routines, trade secret functions, and functions protected by contract (column 1, lines 37-63), McManis is not concerned with the basic software but with certain called routines and so it not concerned with the initial loading of a base application, such as a JVM.

The Patent Office (page 6, lines 7-15, of the Office Action mailed July 1, 2005) further asserts “However, McManis discloses that every file, including the primary files, contains a digital signature and that the digital signature is necessary to verify the authenticity of every called file before that file is loaded (McManis, col. 1, line 65 – col. 2, line 44). It would have been obvious to one of ordinary skill in the art to arrange, at the time of initialization, for the loader program to initially verify the digital signature of the primary file and initially load the primary file. This would have been obvious because one of ordinary skill in the art would have been motivated to verify the authenticity of the primary file, as taught by McManis, when the primary file is initially loaded – so as to protect the system’s integrity at all times.”

Applicant, in response to the above paragraph, again asserts that McManis does not disclose loading and does not disclose loading as being part of the verification process. McManis does not disclose that the primary file is verified by a loading program. McManis discloses a mutual verification process where a calling application verifies the digital signature of a called application and the called application verifies the digital signature of the calling application (e.g., Figure 2). The first problem McManis addresses concerns the isolation of cryptographic routines to prevent the export of sensitive technology (column 1, lines 37-57) so McManis would not be directed to the verification of a basic Java virtual machine, but at cryptographic routines that

might be called by the JVM. The second problem McManis addresses concerns the situation where there is a desire to limit or prevent use of dynamically linkable modules so as to protect trade secrets or provide protection for contractual reasons so McManis would also not be directed to verification of a basic Java virtual machine.

Thus, it is respectfully requested that the Patent Office allow claims 1, 2, 5-8, and 11-13 for these reasons.

Claim 2 recites “The verification system of claim 1, further characterised by at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, **wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file.**”

Claim 8 recites “The verification method of claim 7, further characterised by including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, the method comprising the further steps of **after successful verification and selective loading of the at least one secondary file; using the at least one secondary file to manage the verification and selective loading of the at least one tertiary file.**”

The Patent Office asserts “Regarding claim 2, the modification of McManis discloses: *the plurality of files including at least one tertiary file referenced by at least one secondary file of the plurality of secondary files, wherein after successful verification and selective loading of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file* (McManis, fig. 1, elems. 118, 120; col. 3, lines 12-21, 30-37). McManis discloses that each file can contain a plurality of procedure calls to other files, thus a secondary file may call a tertiary file.”

Applicant asserts that McManis does not disclose or suggest the limitation “wherein after successful verification and selective loading of one of the at least one secondary file, the at least one secondary file is arranged to manage the verification and selective loading of the at least one tertiary file.” Even if column 3, lines 12-21 and 30-37, figure 1, and elements 118 and 120 of McManis could be construed to as a suggestion for a tertiary file, McManis does not disclose or suggest that “at least one secondary file is arranged to manage the verification and **selective loading** of the at least one tertiary file.” Thus, it is respectfully submitted that claims 2-6 and 8-

S.N.: 10/050,083
Art Unit: 2137

12 are allowable for this additional reason.

Claim 5 recites “The verification system of claim 2, further **comprising at least one administrator-configurable file** and characterised by the digital signature key comprising a number of keys including a private key provided by an administrator, **wherein the loader program is further arranged to verify the digital signature of the at least one administrator-configurable file using the private key.**”

Claim 11 recites “The verification method of claim 8, further **comprising at least one administrator-configurable file** and characterised by the digital signature key comprising a number of keys including a private key provided by an administrator, **wherein the loader program is further arranged to verify and selectively load the digital signature of the at least one administrator-configurable file using the private key.**”

The Patent Office asserted (page 7, lines 4-13) “Regarding claim 5, the modification of McManis discloses that all files contain digital signatures so that they may be verified with a digital signature key (McManis, col. 2, lines 22-37). McManis further discloses that verifiable files may contain a number of portions, including a methods portion and a data portion. Each portion is verified by a separate digital signature (McManis, col. 4, lines 54-67). Thus, McManis discloses the digital signature key used to verify the file as being a combination of keys. These verifiable files are often authored, maintained, or updated (“administered”) by others (“administrators”), which is why they are linked dynamically during program execution (McManis, col. 1, lines 10-27). Thus, the modification of McManis discloses at least one of the files as being an administrator configurable file.”

Applicant asserts that McManis contains no teaching or suggestion of the limitation “wherein the loader program is further arranged to verify the digital signature of the at least one administrator-configurable file using the private key” and does not disclose an “administrator-configurable file.” Thus, it is respectfully submitted that claims 5, 6, and 11 are allowable over the prior art of record.

Claim 6 recites “The verification system of claim 5, further characterised by **the software installation being a Virtual Machine installation.**”

Claim 12 recites “The verification method of claim 8, further characterised by **the software installation being a Virtual Machine installation.**”

The Patent Office asserts “Regarding claim 6, the modification of McManis does not disclose that the system is a Java Virtual Machine installation. However, the system of McManis, assigned to Sun Microsystems, Inc., is disclosed as being operable on “virtually any type of computer”, including architecturally distinct systems such as Sun workstations, IBM compatible computers, and Macintosh computers. It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to employ a virtual machine installation such as Java in the system of McManis. This would have been obvious because one of ordinary skill in the art would have logically recognized that a virtual machine installation such as Java would allow the system of McManis to be employed on such a diverse and distinct set of architectures.”

Applicant asserts that McManis does not disclose or suggest a Virtual Machine software installation, as found in claims 6 and 12. It is respectfully submitted that the amendment of Claims 6 and 12 does not introduce new matter and respectfully requested that the Patent Office withdraw its rejection of these claims under 35 U.S.C. 103(a).

The Patent Office rejected claims 3, 4, 9, and 10 under 35 U.S.C. 103(a) as being unpatentable over McManis, “System and Method for Protecting Use of Dynamically Linked Executable Modules,” U.S. Patent No. 5,757,914, in view of Menezes et al., Handbook of Applied Cryptography.

Claim 3 recites “The verification system of claim 2, further characterised by the digital signature key being a public key obtained via the internet.”

Claim 9 recites “The verification method of claim 8, further characterised by the digital signature key being a public key obtained via the internet.”

The Patent Office asserted

Regarding claim 3, the modification of McManis discloses the use of a public key as a digital signature key (McManis, col. 3, lines 38-50). He does not disclose that the public key is obtained from the internet.

Menezes et al. discloses the key management techniques used to share keying material (Menezes et al., pages 543, 544). In public-key systems, entities requiring public keys obtain the public keys via an internet (“inter network”) of certification authorities, key servers, and key management facilities (Menezes et al., pages 548-550).

It would have been obvious to one of ordinary skill in the art to employ the method Menezes et al. for obtaining public keys via an internet with the system of McManis for using a public digital signature key. This would have been obvious because one of ordinary skill in the art would have been motivated to efficiently utilize system

resources by having the public key be obtained from a remote source instead of the program modules themselves generating the public/ private key pairs.

Menezes is concerned with key management techniques and does not disclose a loader arranged to obtain a digital signature key and further arranged to load the primary library file, as claimed. Since McManis is concerned with preventing use or export of certain cryptographic routines, trade secret functions, and functions protected by contract (column 1, lines 37-63), McManis is not concerned with the basic software but with certain called routines and so it not concerned with the initial loading of a base application, such as a JVM. Thus, the combination of McManis and Menezes do not make claims 3 and 9 allowable because of their dependence from allowable base claim 1 and allowable intervening claim 2 and allowable base claim 7 and allowable intervening claim 8, respectively.

Claim 4 recites “The verification system of claim 2, further characterised by the digital signature key being a hidden public key internal to the loader program, **the loader program being arranged to use the hidden public key in the event that a public key cannot be obtained via the internet.**”

Claim 10 recites “The verification method of claim 8, further characterised by the digital signature key being a hidden public key internal to the loader program, **the loader program being arranged to use the hidden public key in the event that a public key cannot be obtained via the internet.**”

The Patent Office asserted

Regarding claim 4, the combination of McManis and Menezes et al. discloses: *the digital signature key being a hidden public key internal to the loader program, the loader program being arranged to use the hidden public key the event that a public key cannot be obtained via the internet* (McManis, col. 4, lines 7-53). The combination of McManis and Menezes et al. shows that public keys used for digital signature generation would be obtained from an internet. The loader program obtains the public key and inherently stores the key internally (as would be required in order to perform the processing of the digital signatures), thus using the obtained key even if it couldn't be obtained by the loader program from an internet.

Both McManis and Menezes are silent regarding a hidden public key and neither disclose or suggest the limitation “the loader program being arranged to use the hidden public key in the

S.N.: 10/050,083
Art Unit: 2137

event that a public key cannot be obtained from the internet". Furthermore, McManis' discloses an embedded public key, but does not suggest or disclose both a hidden public key and a public key obtained via the internet. Thus, claims 4 and 10 are allowable for this additional reason.

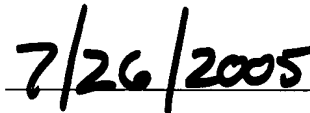
The Examiner is respectfully requested to reconsider and remove the rejections of the claims 1, 2, 5-8, and 11-13 under 35 U.S.C. 103(a) based on McManis, U.S. Patent No. 5,757,914, and of the claims 3, 4, 9, and 10 under 35 U.S.C. 103(a) based on McManis, U.S. Patent No. 5,757,914, in view of Menezes et al., Handbook of Applied Cryptography, and to allow all of the pending claims 1-13 as now presented for examination. An early notification of the allowability of claims 13 is earnestly solicited.

Respectfully submitted:



Harry F. Smith

Reg. No.: 32,493



Date

Customer No.: 29683

HARRINGTON & SMITH, LLP

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: hsmith@hspatent.com

CERTIFICATE OF MAILING

S.N.: 10/050,083
Art Unit: 2137

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

7/26/05 Ann O'Brien-Towill
Date Name of Person Making Deposit



Marked Up Copy

1/2

FIG. 1

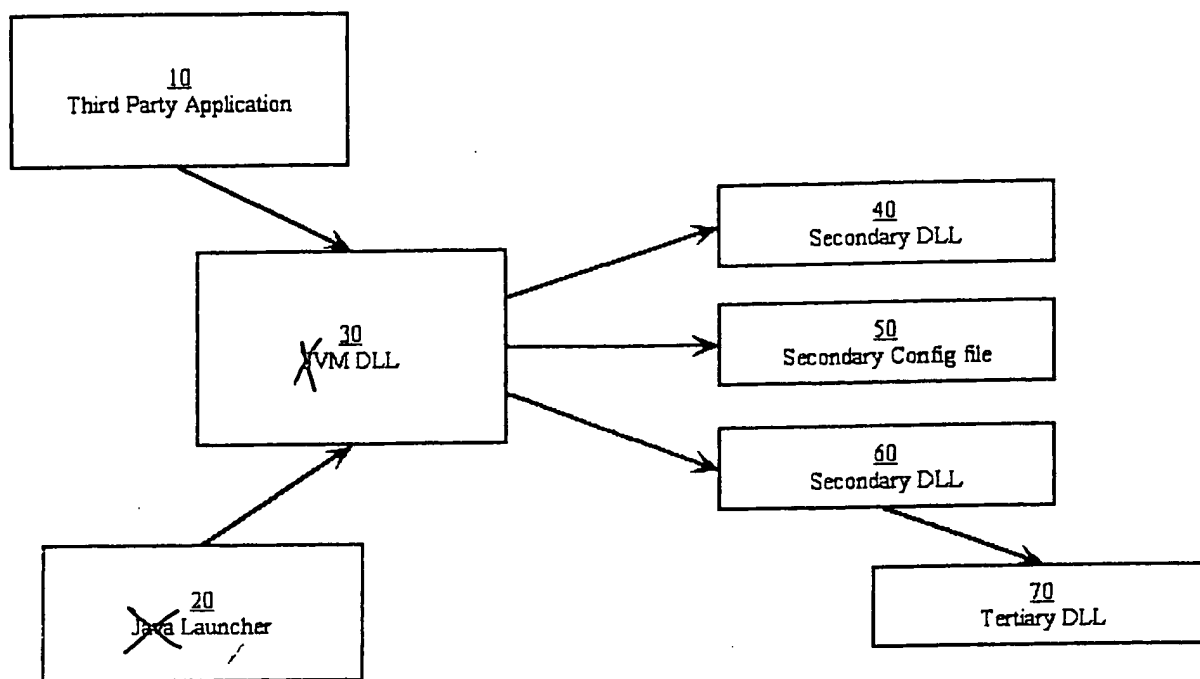


FIG. 2

